Attorney Docket No. GENSP151C1

DISPLAY UNIT STORING AND USING A CRYPTOGRAPHY KEY

Inventors

Osamu Kobayashi 1431 Ormsby Drive Sunnyvale, CA 94087 Citizenship: Japan	Ali Noorbakhsh 116 Shadow Creek Court Danville, CA 94506 USA Citizenship: USA
Chia-Lun Hang 15727 Casino Rea Morgan Hill, CA 95037 Citizenship: USA	Jih-Hsien Soong 21712 Columbus Avenue Cupertino, CA 95014 USA Citizenship: USA
Tzoyao Chan 20237 Marillt Court Saratoga, CA 95070 Citizenship: USA	

Assignee:
Genesis Microchip Corporation
2150 Gold Street Alviso, CA 95002
Phone Number: (408)262-6599

BEYER WEAVER & THOMAS, LLP
P.O. BOX 778
BERKELEY, CA 94704-0778
(650) 961-8300

DISPLAY UNIT STORING AND USING A CRYPTOGRAPHY KEY

Related Applications

[0001] This application is a continuation of U.S. Application No. 09/652,415, filed August 31, 2000 entitled "Display Unit Storing and Using a Cryptography Key" which claims priority from U.S. Provisional Application Serial Number 60/184,999, Entitled, "Display Unit Storing and Using a Cryptography Key", filed on February 25, 2000, which are hereby incorporated by reference.

Background of the Invention

Field of the Invention

[0002] The present invention relates to display units used with cryptography technologies, and more specifically to a method and apparatus for storing and using a cryptography key.

Related Art

[0003] Display units are often used to receive and display data encoded in a display signal received on a serial communication channel. As used in the present application, display units contain both analog display units (typically based on cathode ray tube technology) and digital

[0004] display units (typically based on flat panels). The display signal generally contains data representing image frames and synchronization signals (e.g., VSYNC and HSYNC) indicative of the line and frame boundaries.

[0005] It may be necessary to implement cryptography applications in display units. In a common cryptography application, underlying data is encrypted at a sending location and transferred to a receiving location. The encrypted data is then decrypted at a receiving end to recover the original data. Due to the encryption and decryption, an unauthorized third party may be unable to decipher (or even alter) the underlying data when the data is transmitted from the sending location to the receiving location.

[0006] One common application of cryptography is when a display unit needs to decrypt data encoded in a received display signal. The data is typically encrypted to avoid illegal copying of the data when the display signal is being transmitted. For example, a graphics controller of a computer system may encrypt data representing image frames and send the encrypted data in a serial communication channel, and it may be necessary to decrypt the data in the display unit so that the image frames can be displayed.

[0007] Keys are commonly used in cryptography. Examples of such keys include an encryption key used to encrypt data, a decryption key to decrypt the data, and an authentication key to authenticate the source sending data. Details of guidelines (standards) for implementation of cryptography are provided in further detail in a document entitled, "High Bandwidth Digital Content Protection System, Revision 1.0" dated February 17, 2000, and available from Digital Display Working Group (DDWG), which is incorporated in its entirety herewith.

[0008] Preventing unauthorized access to keys used in cryptography is often important. For example, the encrypted data can often be decrypted by an unauthorized party if the party has access to the decryption key. Therefore, what is needed is a method and

apparatus which prevents (or substantially discourages) unauthorized access to keys.

Summary of the Invention

[0009] An aspect of the present invention provides a secure way of storing and using keys. The keys are stored in encrypted format in a non-volatile memory. The key in the unencrypted form is referred to as an 'unencrypted key' and the key in the encrypted form is referred to as an `encrypted key'. When the key is to be used, an integrated circuit retrieves the encrypted key from the non-volatile memory, decrypts the key and then uses the decrypted key (which equals the unencrypted key). For example, the integrated circuit may retrieve an encrypted authentication key from the non-volatile memory, decrypt the authentication key, and then use the decrypted authentication key for authentication.

[0010] As the keys are stored in encrypted format, an unauthorized user may not be able to decipher the keys by examining the non-volatile memory. In addition, as the key is in encrypted format when retrieved from the non-volatile memory, the key may not be deciphered merely by examining (probing) a bus on which the key is retrieved from the non-volatile memory. Furthermore, as the key is decrypted within an integrated circuit which uses the key, access to the key is further restricted.

[0011] A display unit provided according to an aspect of the present invention may thus contain a non-volatile memory (e.g., EEPROM). A master block (external to the display unit) may be used to generate a key, and the key is provided to the display unit. An encryption circuit encrypts the key according to a protocol and stores resulting encrypted key in the non-volatile memory.

[0012] A decryption circuit within the display unit then retrieves the encrypted key, decrypts

the key, and uses the decrypted key. The decrypted key may be used for authenticating any subsequently received data. As another example, the decrypted key may be used as a decryption key for decrypting any subsequently received data in a way well known in the relevant arts.

[0013] Using the above approach, a component provider may provide a monolithic integrated circuit which contains the encryption and decryption circuits. An OEM (original equipment manufacturer) may provide a key to the encryption circuit, which encrypts the key and stores the encrypted key in a non-volatile memory. When the key is required, the encrypted key is retrieved and decrypted.

[0014] Accordingly, a provider may manufacture similar monolithic integrated circuits for many OEMs, and the OEMs may store OEM specific keys in the display units. The keys need not be shared with the providers of the monolithic integrated circuits. As a result, the OEMs may ensure the availability of the key without the fear of comprising security by sharing the keys with the providers.

[0015] Therefore, an aspect of the present invention is particularly useful for OEMs as the OEMs may provide keys to the units without having to share the keys with the component providers.

[0016] An aspect of the present invention makes it difficult for an unknown third party to access keys as the keys are stored in an encrypted form in a non-volatile memory and the key may be retrieved from the memory only in encrypted form.

[0017] Another aspect of the present invention makes it difficult for an unknown third party to

access the keys as the key may be available in decrypted form only within the integrated circuits during actual use.

[0018] Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

Brief Description of the Drawings

The present invention will be described with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a computer system implemented in accordance with the present invention;

Figure 2 is a block diagram the manner in which a key can be stored and used in accordance with the present invention;

Figure 3 is a block diagram illustrating a display unit implemented in accordance with the present invention; and

Figure 4 is a flow-chart illustrating a method in accordance with the present invention.

Detailed Description of the Preferred Embodiments

1. Overview and Discussion of the Invention

[0019] The present invention is described in the context of a display unit which stores one or more keys in encrypted format ("encrypted key") in a non-volatile memory. When the key is to be used, an integrated circuit retrieves the encrypted key from the non-volatile memory, decrypts the key and then uses the decrypted key. For example, the integrated circuit may retrieve an encrypted authentication key from the non-volatile memory, decrypt the authentication key, and then use the authentication key for authentication.

[0020] As the keys are stored in encrypted format, an unauthorized user may not be able to decipher the keys by examining the non-volatile memory. In addition, as the key is in encrypted format when retrieved from the non-volatile memory, the key may not be deciphered merely by examining (probing) a bus on which the key is retrieved from the non-volatile memory. Furthermore, as the key is decrypted within an integrated circuit which uses the key, access to the key is further restricted.

[0021] The present invention is described below with reference to several examples for illustration. One skilled in the relevant art, however, will readily recognize that the invention can be practiced in other environments without one or more of the specific details, or with other methods, etc. In other instances, well-known structures or operations are not shown in detail to avoid obscuring the invention.

2. Example Environment

[0022] In general, the present invention can be implemented in any display unit, for example, used in conjunction with computer systems, DVD Players, HDTV televisions, etc. However, the invention is described below with reference to computer systems for

illustration. A computer system may be one of, without limitation, lap-top and desk-top personal computer systems, work-stations, special purpose computer systems, general purpose computer systems, network computers, and many others. The invention may be implemented in hardware, software, firmware, or combination of the like.

[0023] Figure 1 is a block diagram of computer system 100 illustrating an example environment in which the present invention can be implemented. Computer system 100 includes central processing unit (CPU) 110, random access memory (RAM) 120, one or more peripherals 130, graphics controller 160, and digital display unit 170. CPU 110, RAM 120 and graphics controller 160 are typically packaged in a single unit, and such a unit is referred to as source 199 as the unit generates and transmits a sequence of symbols on a serial communication channel. All the components in graphics source 199 of computer system 100 communicate over bus 150, which can in reality include several physical buses connected by appropriate interfaces.

[0024] RAM 120 stores data representing commands and possibly pixel data elements representing a source image. CPU 110 executes commands stored in RAM 120, and causes different commands and pixel data elements to be transferred to graphics controller 160. Peripherals 130 can include storage components such as hard-drives or removable drives (e.g., DVD drive, floppy-drives). Peripherals 130 can be used to store commands and/or data which enable computer system 100 to operate in accordance with the present invention. By executing the stored commands, CPU 110 provides the electrical and control signals to coordinate and control the operation of various components in graphics source 199.Graphics controller 160 receives data/commands from CPU 110, and generates pixel data elements representative of source images to be displayed on digital display unit. Graphics controller 160 then encodes the data as symbols in a serial communication channel. The symbols may be sent in an encrypted format. The resulting signal ("display signal") may contain synchronization

signals also in addition to the data. The display signal may be transferred according to standards such as Digital Flat Panel (DFP) and Digital Video Interface (DVI) well known in the relevant arts.

[0025] Display unit 170 may receive a display signal in TMDS format from graphics controller 160, and displays the source images encoded in the display signal. As the symbols (data) may be encoded in an encrypted format, display unit 170 first decrypts the symbols to recover the pixel data elements representing a source image. The corresponding source images are then displayed. The display unit may provide for authentication also. As is well known, decryption and authentication type acts require keys.

[0026] As described below in further detail, the present invention enables the keys to be stored in a non-volatile memory while minimizing the risk that an unknown third party can access the keys. The components of the digital display unit as relevant to the present invention are described below in further detail. The details of display unit are then described in further detail. For further details on the operation of the components, the reader is referred to the co-pending application serial Number: 09/406,332; Filing Date: September 27, 1999, entitled, "Receiver to Recover Data Encoded in a Serial Communication Channel", which is incorporated in its entirety herewith.

3. Use of Key

[0027] Figure 2 is a block diagram of apparatus 200 illustrating the manner in which keys are stored and used in accordance with the present invention. Apparatus is shown containing printed circuit board (PCB) 299 and master block 210. PCB 299 (or parts thereof) are referred to as components which are provided by component providers such as Genesis Microchip Corporation (the assignee of the present application). OEMs (original equipment manufacturers) such as Sony Corporation and Compaq Corporation integrate such

components into units such as display units.

[0028] In operation, an OEM uses master block 210 to provide keys ("encrypted keys") to printed circuit board (PCB) 299. The keys may be generated either internal or external to master block 210, and may be provided in an unencrypted format. The key may be provided in unencrypted form to PCB 299 using VC protocol well known in the relevant arts. As described below in further detail, PCB 299 stores the key(s) in an encrypted form/format ("encrypted key") in a non-volatile memory, and decrypts the keys when required for use.

[0029] PCB 200 may contain monolithic integrated circuit 201, pin header 211, EEPROM 250, micro-controller 260 and DVI (digital video interface) connector 270. Integrated circuit 201 is in turn shown to contain RAM 220, key encryption circuit 230, port 240, the High-bandwidth Digital Content Protection (HDCP) engine 290 (containing key decryption circuit 295 and data decryption circuit 296), and receiver 285. Each component is described below in further detail.

[0030] Pin header 211 may contain two pins (consistent with 1^2C protocol) and provides the physical interface to communicate with master block 210. The data received by pin header 211 includes keys which are stored and used in accordance with various aspects of the present invention.

[0031] Port 240 receives an unencrypted key and places the key in random access memory (RAM) 220, which can also be implemented as multiple registers. Key encryption circuit 230 encrypts the key according to an encryption protocol and stores the encrypted key in RAM 280. The encrypted key can be written directly into serial EEPROM 250 by key check and encrypt 230 if such a feature is available. Alternatively, master block 210 may retrieve the encrypted key from RAM 280, and write the encrypted key into serial EEPROM 250.

[0032] One problem with the above embodiment is that an unauthorized third party may retrieve the encrypted key multiple times and attempt to decipher the unencrypted key. To discourage such attempts, support for multiple encryption/decryption protocols (for

encrypting the keys) may be provided within integrated circuit 201, and the keys may be encrypted according to one of the protocols. The OEM may specify the specific protocol by using appropriate commands. The data indicating the specific protocol may also be stored thereafter in serial EEPROM 250 to facilitate later decryption by HDCP engine 290.

[0033] As a further deterrent against unauthorized deciphering of the keys, the OEM may be required to provide a secret key (generated based on a protocol provided by the component manufacturer), and the appropriate encrypted key may be provided only if the secret key is deemed to authenticate the OEM. As a result, third parties may be unable to access or decipher the keys stored and used in accordance with the present invention.

[0034] Using the noted approaches of above, several keys may be written into EEPROM 250. For example, the keys may include authentication key and a decryption key. The manner in which these keys are used is described below in further detail. DVI connector 270 may receive any cryptography related commands from graphics controller using, for example, ^{12C} protocol on path 272. As an illustration, DVI connector 270 may receive a request to authenticate along with any necessary parameters. The authentication request is passed to HDCP engine 290 in integrated circuit 201. HDCP engine 290 retrieves the encrypted authentication key from serial EEPROM 250 via RAM 220, and decrypts it according to a corresponding decryption algorithm.

[0035] The decrypted authentication key can be used to provide a response to the authentication request. Once the authentication key is decrypted, the response to the authentication can be generated in a known way. Path 272 may be used to implement the communication for the authentication.

[0036] DVI connector 270 is shown connected to two paths, VC path 272 and display signal path 271. 1^2C path 272 may be used to send and receive various security related commands (e.g., authentication sequence as noted above) using the VC well known in the relevant arts. DVI

connector 270 may receive data in encrypted format, for example, from the graphics controller in TMDS format on path 271. The signals are forwarded to receiver 285 in integrated circuit 201. Receiver 285 recovers the data representing the encrypted pixel data element values and forwards the recovered data to HDCP engine 290, which is shown containing data decrypt block 296 and key decrypt block295. Key decryption block 295 receives the decryption key from serial EEPROM 250 via RAM 220, and decrypts the encrypted decryption key according to a decryption algorithm consistent with the encryption algorithm with which the decryption key may have been earlier encrypted. The decrypted key is forwarded to data decrypt block 296. External micro 260 coordinates and controls different components in printed circuit board 299. It should be noted that the decrypted keys are available only in integrated circuit 201, that too only when the circuit is operational. Accordingly, unauthorized third parties may be unable to access the decrypted key even by snooping the buses from which the keys are retrieved from non-volatile serial EEPROM 250. As a result, the keys used in accordance with the present 10invention may be prone less to unauthorized accesses.

[0037] Data decryption block 296 decrypts the data recovered by receiver 285. As the resulting decrypted data represents pixel data elements forming image frames, a display unit may display the images, for example, as described below.

4. Example Display unit

[0038] Figure 3 is a block diagram illustrating an example embodiment of display unit 170. Display unit 170 is shown containing printed circuit board 299, display interface 330, and display screen 350. As described above, printed circuit board 299 receives encrypted pixel data elements from a graphics controller on path 271, and generates the decrypted data on path 297.

[0039] Display interface 330 receives the decrypted data containing pixel data elements on

path 297. Display interface 330 is implemented consistent with the interface requirements of display screen 350. Display screen 350 can be an analog display screen scanned using CRT technology or a flat panel. Alternatively, display screen 350 may be a digital display screen based on flat panel monitor. Display interface 330 generates the corresponding display signals to cause the images represented by the pixel data elements to be displayed on display screen 350.

[0040] Thus, the present invention provides a display unit which enables keys to be stored and used while minimizing the risk of unauthorized access of the keys. A method in accordance with the present invention may be summarized as following.

5. Method

[0041] Figure 4 is a flow chart illustrating a method in accordance with the present invention. The method is described with reference to display unit 170 for illustration. The method starts in step 401 in which control passes to step 410. In step 410, display unit 170 receives a key. In step 420, display unit 170 decrypts the key according to an encryption protocol. As noted above, display unit 170 may be designed to encrypt the key using one of several encryption protocols. In step 430, display unit 170 stores the encrypted key in a non-volatile memory. The non-volatile memory may be located within display unit 170 as described above. In addition, the memory may be implemented with components such as entire memory modules (e.g., EEPROM) or using a small memory units such as registers.

[0042] In step 440, display unit 170 may retrieve the encrypted key when needed. A need arises according to the specific purpose for which the key is designed for. For example, if the key is used for encryption, the key is retrieved prior to decryption of the corresponding data. In step 460, display unit 170 decrypts the key consistent with the encryption protocol used above. In step 470, display unit 170 uses (e.g., for authentication or decryption of data) the decrypted

key. Display unit 170 may retrieve the keys any number of times as indicated by the loop shown in Figure 4.

[0043] Thus, a display unit provided in accordance with the present invention may store any keys in an encrypted form in a non-volatile memory, and decrypt the key only when actually required for use. As a result, the keys may not be easily deciphered and accessed by an unauthorized third party. In addition, it should be understood that steps 410-430 are performed usually by an OEM at the time of assembling the display units, and the loop of steps 440-470 is performed when a end user uses the display unit later.

6. Conclusion

[0044] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.